Plataforma para servicios de facturación y pago en ambientes ubicuos*

Billing and Payment Platform in Ubiquitous Environments**

Plataforma para serviços de cobrança e pagamento em ambientes ubíquos***

*Zeida María Solarte-Astaíza*****
*Óscar Mauricio Caicedo-Rendón******
*Javier Imbuz*******
*Milton Ausecha********

* Fecha de recepción: 10 de diciembre de 2008. Fecha de aceptación para publicación: 16 de abril de 2009. El proyecto está basado en el resultado del trabajo de grado de maestría de los dos últimos autores.

** Submitted on December 10, 2008. Accepted on April 16, 2009. The project is based on the results of the last two authors' MA degree thesis.

*** Data de recepção: 10 de dezembro de 2008. Data de aceitação para publicação: 16 de abril de 2009. O projeto é o resultado do trabalho de mestrado dos últimos dois autores.

**** Ingeniera electrónica. Magíster en Ingeniería, Área Telemática. Profesora, Universidad Autónoma de Occidente, Cali, Colombia. Correo electrónico: zsolarte@uao.edu.co.

***** Ingeniero en Electrónica y Telecomunicaciones. Especialista en Redes y Servicios Telemáticos. Magíster en Ingeniería. Profesor, área de Ingeniería Telemática, Universidad del Cauca, Popayán, Colombia.
Correo electrónico: omcaicedo@unicauca.edu.co.

****** Ingeniero en Electrónica y Telecomunicaciones, Universidad del Cauca, Popayán, Colombia.
Correo electrónico: javier.imbus@gmail.com.

******* Ingeniero en Electrónica y Telecomunicaciones, Universidad del Cauca, Popayán, Colombia.
Correo electrónico: mi1000ton@hotmail.com.

Resumen

La computación ha pasado por dos etapas: la de las computadoras centralizadas con gran poder de procesamiento y la del computador personal. En el horizonte cercano aparece otra etapa, denominada computación ubicua, la cual permite que servicios y aplicaciones residentes en dispositivos móviles o fijos se ejecuten por sí mismos, de acuerdo con el contexto del usuario, y que dichos dispositivos tengan la capacidad y la inteligencia de regular el procesamiento y el intercambio de información según determinadas circunstancias. Esto hace que las tecnologías ubicuas, y obviamente los servicios que sobre ellas se implementan, tengan nuevos retos asociados con la gestión de la seguridad (privacidad, autenticación, autorización, no repudio, etc.), los cuales se incrementan en los mecanismos de pago, pues finalmente estos harán comercialmente viables o no los servicios ubicuos (que están emergiendo con gran fuerza). Por lo tanto, se considera de gran importancia empezar su estudio, concepción, desarrollo, implementación e implantación en Colombia, para tratar de evitar el rezago tecnológico en este campo. Como una primera aproximación a este tipo de servicios en el país, el artículo presenta una plataforma de facturación y pago de servicios en ambientes móviles ubicuos, que permitirá principalmente el estudio y apropiación de los principales aspectos tecnológicos y de seguridad asociados con los sistemas de pago presentes en este tipo de computación, así como su contextualización en el entorno colombiano.

Palabras clave

Computación ubicua, pago—innovaciones tecnológicas, pago—medidas de seguridad.

Abstract

Computing has gone through two stages: the centralized computers with high processing power and personal computers. In the short term, we can see a new stage named as ubiquitous computing, which allows services and applications located within fixed or mobile devices to auto-run according to the context of the user, and that those devices have the ability and intelligence to manage the processing and exchange of information according to the needs of the user. This makes the ubiquitous technologies and services that obviously are implemented on them, include new challenges relating to the security (privacy, authentication, authorization, non-repudiation), that needs to be increased on the payment mechanisms that will decide if the services ubiquitous can be commercially safe and viable. The ubiquitous services are emerging with great force. Therefore, it is considered of great importance to begin the study, design, development, implementation and deploy of these services in our country, and then to try to avoid the technological gap in this field. In order to implement and deploy these services in Colombia, this project provides a platform for billing and payment services in ubiquitous mobile environments, that enable the study of the main technological and safety aspects associated with online payment systems in this kind of computing and how it should work in the Colombian business environment.

Key words

Ubiquitous Computing, payment – technological innovations, payment – safety measures.

Resumo

A computação passou por duas etapas: a dos computadores centralizados com grande poder de processamento e a do computador pessoal. No horizonte próximo aparece outra etapa, denominada computação ubíqua, que permite que serviços e aplicações residentes em dispositivos móveis ou fixos executem-se por si mesmos, de acordo com o contexto do usuário, e que tais dispositivos tenham a capacidade e a inteligência de regular o processamento e o intercâmbio de informação de acordo com determinadas circunstancias. Isto faz com que as tecnologias ubíquas, e obviamente os serviços que se implementem sobre elas, apresentem novos desafios associados à gestão da segurança (privacidade, autenticação, autorização, não repudio, etc.), os quais aumentam nos mecanismos de pagamento, pois finalmente estes farão comercialmente viáveis ou não os serviços ubíquos (que estão emergindo com grande força). Portanto, considera-se de grande importância começar o seu estudo, concepção, desenvolvimento e implementação na Colômbia, para tentar evitar atraso tecnológico nesta área. Como uma primeira aproximação a este tipo de serviços no país, o artigo apresenta uma plataforma de cobrança e pagamento de serviços em ambientes móveis ubíquos, que permitirá principalmente o estudo e apropriação dos principais aspectos tecnológicos e de segurança associados com os sistemas de pagamento presentes neste tipo de computação, bem como a sua contextualização no entorno colombiano.

Palavras chave

Computação ubíqua, pagamento—inovações tecnológicas, pagamento—medidas de segurança.

Introducción

La expresión *computación ubicua* fue introducida por Mark Weiser en 1991. Según este autor, la computación ubicua se describe como computadores muy pequeños con capacidad de comunicación y de computación que se incrustan de forma casi invisible en cualquier tipo de dispositivo cotidiano. Estos dispositivos se encuentran por todas partes y se integran de forma amigable con los humanos, tanto que casi son imperceptibles para ellos (Weiser, 1991).

A pesar del gran avance en cuanto a dispositivos que las personas pueden llevar consigo en todo momento y a las redes inalámbricas que permiten que tales dispositivos puedan formar redes de manera espontánea sin requerir ningún tipo de infraestructura, aún existen retos de investigación para que la computación ubicua y sus servicios sean ampliamente desplegados y aceptados por los usuarios (Davies y Gellersen, 2002).

Dentro de estos aspectos, tienen gran relevancia los modelos económicos y los sistemas de pago asociados, los cuales deben garantizar el retorno a la inversión de manera efectiva, ya que este tipo de servicios no son subsidiados, como lo fue el servicio de internet en sus comienzos, ni son ofrecidos de manera única por grandes operadores, como lo es la telefonía móvil. En este tipo de servicios, dadas sus características, entran en juego muchas más empresas de diferentes tipo y personas de manera individual.

Todos los servicios ubicuos tienen características comunes inherentes a su naturaleza, pero el servicio de facturación y pago es un caso particular con rasgos propios, especialmente en los aspectos de seguridad y confidencialidad de la información, por el tipo de datos manipulados en este tipo de sistemas. Por esto en el proyecto para el desarrollo de la plataforma de facturación y pago se tuvieron en cuenta estas consideraciones desde un principio.

Un sistema de pago en un ambiente ubicuo combina dos situaciones que deben tenerse en cuenta a la hora de definir sus características, las particularidades propias de los ambientes ubicuos y las características de los sistemas de

pago, las cuales deben ser combinadas para obtener un sistema adecuado. En este contexto, y de acuerdo con lo expresado por algunos autores (Boddupalli *et al.*, 2003), las principales características de los sistemas de pago en ambientes ubicuos son:

- Espontaneidad: los mecanismos de pago para servicios ubicuos no deben requerir que los individuos establezcan unas relaciones muy complejas con los proveedores de servicio involucrados en el pago (Boddupalli, 2003).
- Eficiencia: es importante que el sistema de pago sea liviano y eficiente, caracterizado por costos de comunicación y computación bajos, acoplados con recargas financieras mínimas (Juniper Research, 2004).
- Seguridad: un sistema de pago seguro debe tener las siguientes características, propias de cualquier ambiente seguro (Kadhiwal, 2007): confidencialidad, autenticación, integridad, autorización, disponibilidad y no repudio; además, la seguridad en los ambientes ubicuos debe analizarse desde el punto de vista de los dispositivos móviles, las tecnologías de red y la calidad del servicio.
- Flexibilidad: aunque por lo general los ambientes ubicuos se consideran ricos en dispositivos y en redes, se deben tener en cuenta dos situaciones especiales relacionadas con la flexibilidad: la operación sin conexión y la no disponibilidad de los dispositivos (Kadhiwal, 2007).
- Facilidad de uso: se refiere al grado de comodidad y a la utilidad percibida por los usuarios en el momento de usar el sistema de pago ubicuo; es un aspecto crucial si se tienen en cuenta el gran número de transacciones que una persona podría realizar durante el curso de un día normal (Boddupalli, 2003).
- Despliegue: requisito no funcional que se ocupa de la fiabilidad y facilidad con que las aplicaciones se pueden poner en funcionamiento en el entorno de producción (Boddupalli, 2003).

1. Facturación y pago de servicios en ambientes móviles ubicuos

Alrededor de los pagos móviles se han desarrollado gran variedad de proyectos que tienen diferentes características y se enfocan en atacar diversas necesidades, pero hasta el momento no hay ninguna solución integral. Las soluciones de pago existentes no son lo suficientemente seguras, son muy difíciles y lentas de usar o están disponibles solamente para una pequeña cantidad de productos o servicios o para un grupo reducido de clientes. Algunos de estos sistemas o proyectos se describen a continuación:

- *Universal Pervasive Transaction Framework (*UPTF) (Labrou *et al*., 2004): consiste en el desarrollo de una plataforma para trabajar en ambientes invasivos que permite realizar acuerdos entre las diferentes partes de una transacción hecha a través de dispositivos móviles en ambientes inalámbricos inseguros. Se implementaron dentro del proyecto dos sistemas completos para compra y pago a través de dispositivos móviles: en el primero se trabaja con un dispositivo diseñado especialmente para este propósito, mientras el segundo trabaja con teléfonos móviles con soporte a Java ME (*Java Micro Edition*).

- *Paid Peer to Peer M-Payment System (*P2P) (Gao *et al*., 2005): propone un sistema de pago móvil de igual a igual que permite a los usuarios móviles llevar a cabo pagos de manera inalámbrica, a través de tecnología *Bluetooth,* y ejecutar las transacciones hacia el servidor de manera segura.

- *Payment Session Protocol* (PSP) (Boddupalli, 2003): brinda soporte a interacciones relacionadas con pagos entre clientes y servidores en ambientes ubicuos. Refleja transacciones comerciales del mundo real y se basa en el intercambio de contratos, los cuales describen las características no funcionales de los servicios, como calidad del servicio, costos, términos y condiciones de uso. Permite crear acuerdos de servicio entre clientes y servidores. PSP está diseñado para funcionar en conjunto con una solución de pago basada en micropago.

- *PayPal, en línea* (*PayPal*): es un servicio de pago en línea bastante popular, adquirido recientemente por la empresa *eBay*. A través del uso de teléfonos celulares habilitados con sistema WAP, los usuarios pueden usar interfaces inalámbricas de *PayPal* para realizar los pagos. Con el servicio *PayPal Mobile* se puede enviar dinero, comprar artículos o donar desde su dispositivo móvil. Los usuarios de este servicio hacen pagos a través del envío de mensajes de texto a *PayPal*. Este último llama al usuario para confirmar el pago móvil y entonces envía el dinero a la cuenta. En el caso de una compra *Text to Buy*, después de que el comerciante ha recibido el pago, el artículo comprado se envía a la dirección previamente almacenada en la cuenta *PayPal* del usuario.

- *MobyPay* (*Mobypay*, 2008): es uno de los sistemas de pago más versátiles, ya que permite macro y micropagos. Se puede usar para transacciones persona a persona (P2P) o para pagar en el punto de venta (POS), e incluso le da al usuario la opción de escoger entre cargar el servicio a la factura telefónica o usar una tarjeta bancaria (débito o crédito).

- *Secure Mobile Payment Service* (Semops) (Vilmos y Karnouskos, 2003): es un sistema de pago amigable al usuario, universal y complejo. Las posibles transacciones que se pueden realizar con este sistema de pago incluyen pagos en puntos de venta, pagos en línea por internet o WAP, transferencias P2P, compras en máquinas expendedoras y también pagos de facturas; pueden ser micro o macropagos. Para los usuarios y los comerciantes, el servicio de pago es suministrado por su propio banco o por el operador móvil. Como no existen intermediarios involucrados en el proceso, la transacción completa de pago se basa en relaciones de confianza entre las partes. En este sistema, los usuarios no necesitan dar ninguna información sensitiva; por lo tanto, ellos pueden aparecer anónimos durante el proceso de pago. Al recibir la información necesaria de la transacción, el usuario prepara y firma un requerimiento de compra y lo envía a su propio procesador de pago. Si los fondos son suficientes, el comerciante recibe una notificación de pago desde su propio procesador de pago.

El desarrollo del servicio de facturación y pago se orienta a las características de los sistemas de pago en ambientes ubicuos, definidas anteriormente, y al análisis de modelos de pago como los mencionados, con el fin de presentar un modelo integral, que integre de manera sustancial la seguridad y la facilidad de uso. Con este fin se definió una plataforma que permitió la definición y caracterización del servicio de manera detallada, la cual se materializó a través de una arquitectura en la que se implementaron y validaron las características definidas.

2. Plataforma de facturación y pago

Al ser una plataforma de pago, la seguridad es esencial, ya que sin ella los participantes en el servicio no se sentirían cómodos con su uso. La información que se transmite durante todo el proceso debe protegerse de intrusos, debido a la naturaleza crítica de esta; además, es necesario definir políticas de seguridad adecuadas que garanticen la estabilidad, la eficiencia y el control de riesgos, condiciones indispensables en un sistema de pago y exigidos por cualquier entidad financiera involucrada.

Los sistemas de pago por proximidad tienen como característica principal la mínima intervención del usuario y la espontaneidad, lo que permite que el proceso de pago sea muy natural durante su ejecución en el punto de venta, lo cual permite que los productos por los que el usuario está pagando sean de toda índole y no sólo servicios de descarga a través de la web.

Otro factor importante en la caracterización del servicio es que su entorno de ejecución será Colombia, por lo cual debe adaptarse a las condiciones sociales, tecnológicas y legislativas del país. Dadas estas razones, se ha determinado que la plataforma cumpla con las siguientes condiciones:

- Debe poder usarse con teléfonos celulares de gama baja y media, que son los más comunes en Colombia.
- La tecnología de contacto que se usará debe poder adaptarse a este tipo de dispositivos. Se escogió, por lo tanto, la identificación por radiofrecuencia (RFID, por su sigla en inglés) (Moroz, 2004) en dispositivos de gama baja o por *Near Field Communication* (NFC) (Innovission, Research and Technology, 2006) en dispositivos de gama alta.
- La seguridad deberá basarse en certificados y firmas digitales como lo define la ley de comercio electrónico en Colombia (Colombia, Ley 527 de 1999).

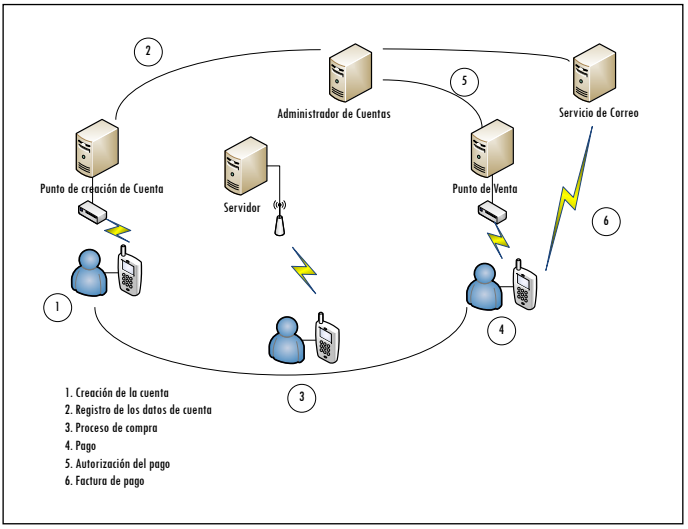
Para simplificar el servicio de pago para los usuarios, este se basará en cuentas bancarias y no en bolsas de dinero digitales, las cuales son menos comunes en el país, y a pesar de que el grado de bancarización no es muy alto en algunos sectores, el gobierno está haciendo un gran esfuerzo por extenderlo (Ministerio de Comercio Industria y Turismo y Bancoldex, 2008).

Para acceder a la plataforma de facturación y pago, el usuario debe contar con una cuenta de servicio en el sistema. En el momento de crearla, en el dispositivo móvil se almacena la información necesaria para realizar los pagos. La cuenta de servicio creada debe tener asociada una cuenta bancaria habilitada para pagos móviles de la cual finalmente se debitan los valores pagados por el usuario.

Antes de acceder a la plataforma de facturación y pago, el usuario debe haber accedido a un servicio ubicuo de compra y, por lo tanto, en su dispositivo móvil y en el punto de venta se encuentra la información de los artículos comprados y del valor que va a pagar. Es importante resaltar que la plataforma propuesta es responsable del proceso de facturación y pago y no del proceso de selección de los artículos y su compra.

En el momento de pagar, el usuario debe acercar su dispositivo móvil al lector que se encuentra en el punto de venta y, de esta manera, sin ninguna otra intervención del usuario, el pago se hará efectivo. Después de realizado el pago, el usuario recibe en su dispositivo móvil un mensaje de texto que le indica que este se realizó exitosamente, mientras la factura de la compra se le envía a través de un mensaje a la cuenta de correo electrónico especificada por el usuario durante el proceso de creación de la cuenta. En la Figura 1 se muestra este proceso.

Figura 1. Proceso de facturación y pago



Fuente: presentación propia de los autores.

2.1 Arquitectura de facturación y pago

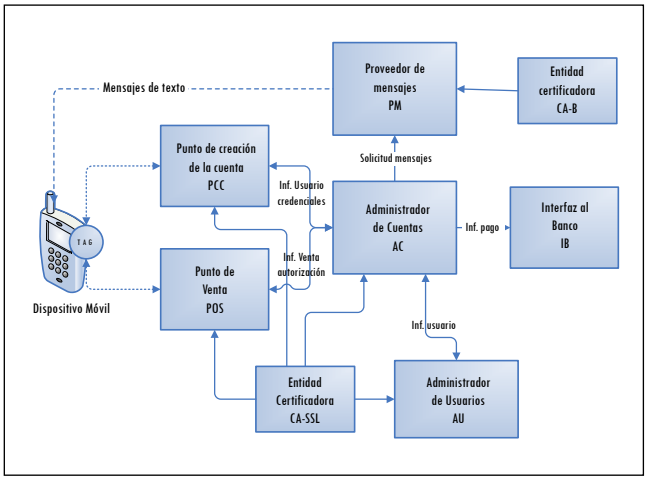
Como se puede observar, la plataforma de facturación y pago es compleja, pues debe cumplir con varios requerimientos (asociados a las cuentas, asociados a los pagos y asociados a la facturación); además, aparecen involucrados varios actores con diversos tipos de relaciones entre ellos. Por esta razón, se decidió adoptar para su desarrollo un análisis basado en arquitecturas de *software* (Albin, 2003).

Con base en la caracterización de la plataforma de facturación y pago y de sus requerimientos, se definieron las siguientes subtareas, a fin de definir la estructura de la arquitectura:

- Creación de las cuentas de usuario.
- Manejo y administración de las cuentas del servicio de facturación y pago.
- Almacenamiento y administración de la información de los usuarios.
- Interfaz con el banco.
- Pago de los productos.
- Envío de mensajes informativos al usuario.
- Envío de la factura digital al usuario.
- Certificación de los participantes en el proceso.
- Firma digital de la factura.

Cada una de las tareas definidas se asoció con un módulo funcional dentro de la arquitectura (Figura 2). La descripción de cada uno de los módulos se presenta a continuación.

Figura 2. Arquitectura general de facturación y pago



Fuente: presentación propia de los autores.

- Dispositivo móvil: es la parte correspondiente al cliente de la arquitectura. A través de este módulo, el usuario interactúa con la plataforma de pago y es aquí donde se almacena la información de las credenciales de la cuenta del usuario. Esto se debe hacer en el elemento seguro del dispositivo (etiqueta RFID/NFC).

- Punto de venta (POS): es el módulo a través del cual el usuario hace efectivo el pago, lee las credenciales almacenadas en el dispositivo móvil y las transfiere al administrador de cuentas.

- Punto de creación de la cuenta (PCC): a través de este módulo el usuario se inscribe al servicio de facturación y pago, y puede realizar funciones como crear una cuenta para la realización de los pagos, bloquearla en caso de robo del dispositivo móvil o cancelarla cuando no se quiera más el servicio.

- Administrador de cuentas (AC): es uno de los módulos más importantes de la arquitectura, ya que establece comunicación con la mayoría de ellos.

Coordina todo el proceso de autenticación y autorización, al igual que genera las credenciales del usuario. En el momento del pago, recibe la información de las credenciales del usuario del punto de venta y se comunica con el banco a través de la interfaz al banco y con el administrador de usuarios para solicitar la autorización del pago.

- Administrador de usuarios (AU): este módulo se constituye en el repositorio de los datos relacionados con la información de los usuarios y sus credenciales, que permite la validación de la identidad de los usuarios en el momento del pago.

- Interfaz al banco (IB): este módulo permite la interacción del módulo "Administrador de cuentas" con el banco que ofrece a los usuarios las cuentas bancarias habilitadas para pagos móviles.

- Proveedor de mensajes (PM): es el encargado de enviar los mensajes de texto y la factura al dispositivo móvil del usuario a solicitud del administrador de cuentas.

- Entidades certificadoras (CA-SSL y CA-B): se encargan de certificar la autenticidad de las entidades que intervienen en el proceso de pago, y para ello les genera certificados y claves.

2.2 Seguridad en la arquitectura

Los aspectos que se tuvieron en cuenta durante la definición de la arquitectura asociados a la seguridad son los siguientes:

- Confidencialidad: las credenciales de la cuenta del usuario permanecen seguras durante todo el proceso, tanto de creación de la cuenta como del pago, ya que la información siempre permanece cifrada.

- Autenticación: la autenticación se realiza con base en certificados digitales.

- Autorización: se realiza en el contexto de la autenticación. Cuando los participantes se autentican de manera satisfactoria, se les permite seguir con los procesos iniciados; en caso de que la autenticación falle, se generan mensajes de error y estos se interrumpen.

- No repudio: la utilización de los certificados digitales y la criptografía de claves públicas para firmar electrónicamente las transacciones y los mensajes se

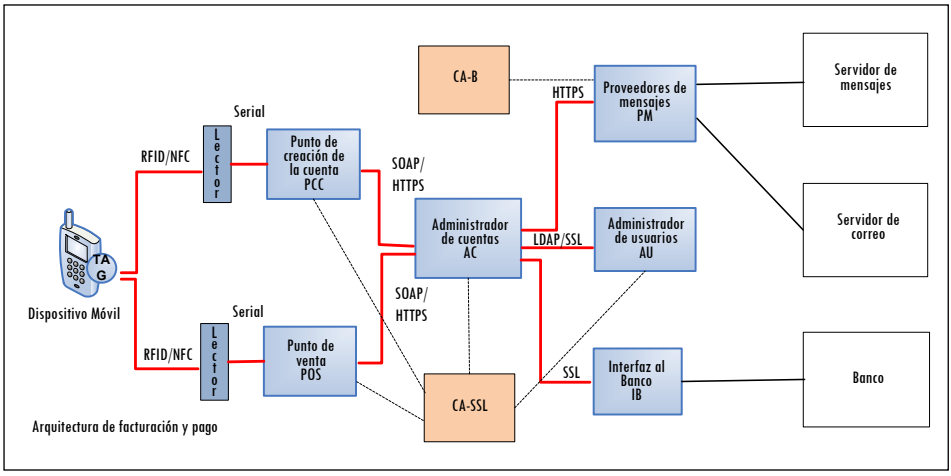
constituyen en pruebas de las transacciones llevadas a cabo. La firma digital de los datos es una prueba suficiente.

El proceso de certificación dentro de la arquitectura de facturación y pago permite que los módulos que deben transferir información sensible se autentiquen frente a los otros y, de esta manera, se garantice su autenticidad. Además, permite que la generación de las claves para cifrar los mensajes se realice también de manera segura. Estos certificados digitales serán emitidos para la autoridad de certificación CA-SSL. Por otro lado, el emisor de mensajes requiere una firma digital para garantizar la autenticidad de las facturas digitales enviadas al usuario, la cual será generada por la autoridad de certificación CA-B.

2.3 Protocolos de comunicación

Dada la importancia de la seguridad en la comunicación entre los módulos que componen la arquitectura de facturación y pago, en la Figura 3 se presentan los tipos de protocolo implementados entre ellos.

Figura 3. Protocolos de comunicación



Fuente: presentación propia de los autores.

La Tabla 1 resume los aportes y las características de cada protocolo dentro de la arquitectura de facturación y pago.

Tabla 1. Aportes a la arquitectura de facturación y pago de los protocolos de comunicación

Protocolo	Aportes	Características
RFID/NFC	• Proximidad • Interoperabilidad • Seguridad	• Permite tener una comunicación de corto alcance, lo que le da la característica de proximidad al sistema de pago • Está basado en estándares que permiten la interoperabilidad • Implementa algoritmos para asegurar la comunicación
SERIAL (Assa Abloy, 2006)	• Acceso a datos en la etiqueta • Configuración de la comunicación • Seguridad	• Permite el acceso desde la aplicación a los datos de la etiqueta RFID a través del lector • Permite la configuración de la comunicación entre la etiqueta y el lector, para hacerla segura • Permite el cifrado de la información con grados de seguridad adecuados
SOAP (Massachusetts Institute of Technology, 2001)	• Interoperabilidad	• Permite la comunicación sobre protocolos estándares, como HTTP con fines de interoperabilidad
HTTPS	• Seguridad • Autenticación • Integridad	• Brinda seguridad en la comunicación a través del cifrado de datos basado en *Secure Socket Layer* (SSL) • Permite la autenticación, tanto de clientes como de servidores, y garantiza la integridad de la información a través de una infraestructura de claves públicas
LDAPS (Hodges y Morgan, 2002)	• Acceso a datos almacenados • Optimización • Seguridad	• Permite el acceso a los datos almacenados en el sistema de directorio • Optimiza el proceso de búsqueda de información, lo que permite que las operaciones de lectura de datos para la validación sean rápidas • Ya que corre sobre HTTPS hace que el acceso a la información sea seguro

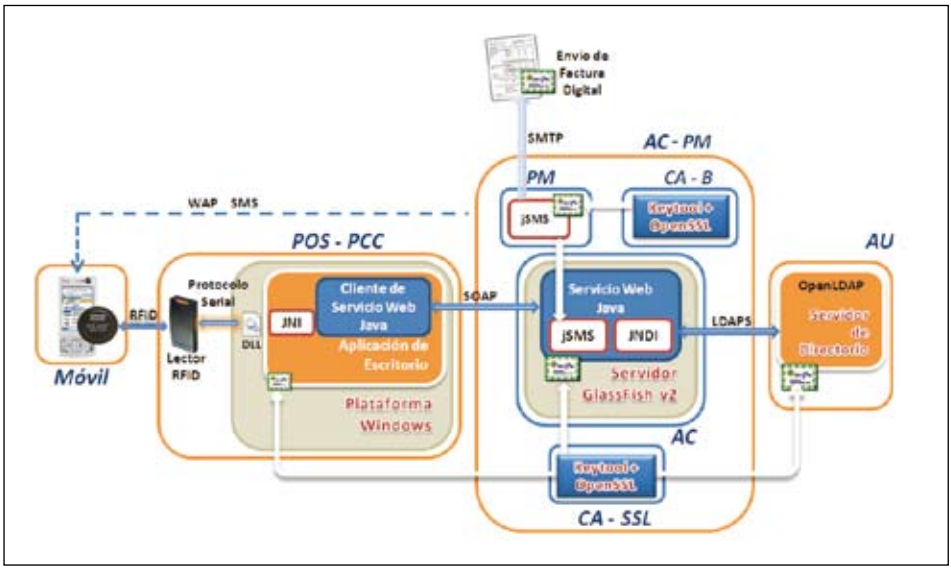
RFID: identificación por radiofrecuencia; *NFC: Near Field Communication*; SOAP: *Simple Object Acces Protocol*; HTTPS: *HiperText Transfer Protocol Secure*; LDAPS: *Lightweight Directory Access Protocol over SSL*.
Fuente: presentación propia de los autores.

3. Implementación y pruebas de la arquitectura de facturación y pago

La Figura 4 muestra el diagrama de implantación de la arquitectura. Para usar de mejor manera los recursos computacionales se montaron varios módulos de

la aplicación sobre el mismo servidor físico. Luego se describen las tecnologías y herramientas utilizadas para la implementación de cada componente:

Figura 4. Diagrama de implantación



Fuente: presentación propia de los autores.

- *AC*: el AC se compone de un servicio web seguro implementado en *Java*. Se desplegó en el servidor de aplicaciones *GlassFish v2*, que se basa en el sistema METRO (Collabnet, 2007). El servidor se implantó en una estación con sistema operativo *Debian Etch 4.0* y *Java 2 SE*. El servicio web desarrollado usa el API *JNDI*, para utilizar el *Lightweight Directory Access Protocol over SSL* (LDAPS). El servicio web se comunica con sus clientes mediante el protocolo *Simple Object Acces Protocol* (SOAP 1.1), definido en (Massachusetts Institute of Technology, 2001). Debido a que el banco se simuló como una base de datos de *MySQL 5.0*, la capa de adaptación del AC con el banco se realizó con *DAO* mediante *FREE DaoGen generator*, versión 2.4.1 (DAO, en línea).

- *PM*: para el envío de los mensajes SMS se utilizó *ObjectXP jSMS 2.2.1* (Object XP, 2006). *jSMS* es un API escrito en *Java*, que se integra muy fácilmente con el servicio *web* seguro del AC; también se utilizó para el envío de la factura digital firmada a la cuenta de correo del usuario luego de realizar una compra.

- *CA-SSL y CA-B*: las herramientas para realizar la generación de certificados, de llaves y de *keystores* son *Java Keytool* y *OpenSSL 0.9.8c*.

- *AU*: se usó un servicio de directorio montado con *OpenLDAP-2.3.39*, que corre sobre una estación con *Debian Etch 4.0* y que se comunica con el AC a través de *LDAPS* (Hodges y Morgan, 2002). La ruta donde *OpenLDAP* guarda su directorio en una base de datos de tipo *Oracle Berkeley v 4.4.,* la versión más estable para realizar la compilación.

- *POS* y *PCC*: están montados bajo el mismo esquema, es decir, *Debian Etch*, *JavaSE* y una aplicación *Java* de escritorio, que cuenta con la característica de ser un cliente de servicio web seguro y comunicarse con un lector RFID. El lector RFID es del fabricante HID, referencia *iCLASS RW100/6101 BKV000*. La aplicación *Java* de escritorio que se implementa en estos módulos se comunica con el lector RFID mediante la implementación del protocolo serial *iCLASS v2.4* (Assa Abloy, 2007), a través de un puerto USB con el API JNI.

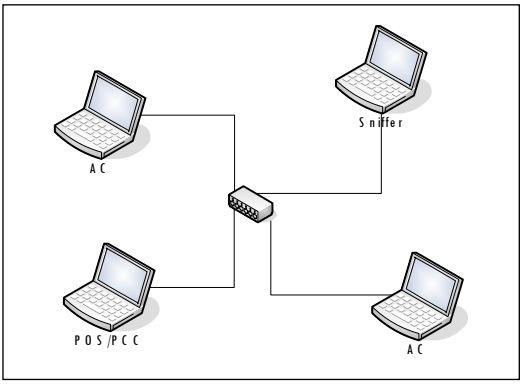
- *Móvil*: se utilizaron etiquetas RFID HF, ya que cuentan con mayor capacidad de almacenamiento, son más económicas, permiten una alta tasa de transmisión de datos a distancias cortas, manejan estándares consolidados como el ISO 14443, garantizan interoperabilidad entre dispositivos y soportan cifrado de datos con algoritmos como *DES y3DES* (Moroz, 2004).

Dado que la seguridad es uno de los aspectos críticos de la arquitectura, a continuación se detalla el proceso seguido para determinar sus grados de seguridad. La topología de la red utilizada para las pruebas es la mostrada en la Figura 5, donde se emplearon tres equipos para la simulación del servicio y otro más para realizar los ataques.

Basado en los posibles ataques se desarrollaron pruebas en los siguientes aspectos:

- Pruebas de *scanning*. Estas pruebas permiten detectar los puertos abiertos en un equipo. Los servidores AC y AU fueron sometidos a esta prueba, y aunque es un procedimiento pasivo e inofensivo, permitió detectar la facilidad con la cual se accede a la información y que después puede convertirse en el primer paso de un ataque que concluya con la deshabilitación de cualquiera de los dos servidores. Por lo anterior, es importante y fundamental instalar un *firewall* que impida este tipo de ataques y así bloquear cualquier tipo de amenaza desde el principio.

Figura 5. Topología de la red de pruebas



Fuente: presentación propia de los autores.

- Pruebas de *sniffing*. Estas pruebas permiten el monitoreo y análisis del tráfico que se cursa en el sistema. Al capturar la información que se transmite entre el AC y el AU se pudo observar que esta información estaba cifrada, lo que hace imposible visualizar los datos transferidos y las operaciones que se llevan a cabo, debido al manejo de certificados y del protocolo TLS en el servidor. El mismo tipo de pruebas se realizaron entre el AC y el POS/PCC.

- Pruebas de *spoofing*. Se trata de una técnica de ataque consistente en suplantar a una entidad de una red con el fin de recibir información confidencial. Las dos entidades escogidas para esta prueba fueron el AC y el AU, y se utilizó una herramienta que permitió la suplantación del AU. Al hacer la prueba se detectó que a pesar de que la información se transmite de manera cifrada, el suplantador, además de interceptar los datos, los recibe incluyendo llaves de seguridad, por lo cual con las herramientas y algoritmos suficientes se podría descifrar la información. Para solucionar este riesgo de seguridad se implementó una red privada virtual (VPN, por su sigla en inglés) que impide la conexión de intrusos a equipos del servicio al solicitar una autenticación inicial.

- Pruebas de denegación de servicio. La denegación del servicio consiste en interrumpir la comunicación y así alterar su prestación. Para esta prueba se intentó acceder al directorio LDAP del AU desde el AC y el resultado fue el no acceso al servidor. También se realizó la inserción de datos en la comunicación, lo que

facilita la generación de una sobrecarga en el enlace, otra forma de este tipo de ataque. Aunque el desenlace es diferente al del ataque *spoofing*, el origen es el mismo, esto es, la ausencia de un mecanismo robusto de autenticación que impida la suplantación de una entidad, por lo cual la solución también es una VPN.

- Pruebas de *exploits*. Un *exploit* es un programa que aprovecha una vulnerabilidad de un equipo para alterar el funcionamiento de un servicio o aplicación. Al atacar los servidores AC y AU se obtuvieron buenos resultados de seguridad, es decir, ninguno de los *exploits* tuvo éxito. Sin embargo, así actualmente no se encuentren *exploits* que afecten la arquitectura, en cualquier momento puede aparecer una amenaza para este sistema, por lo cual es importante evitar este tipo de ataques a través de *firewalls*.

4. Análisis de la seguridad de la arquitectura

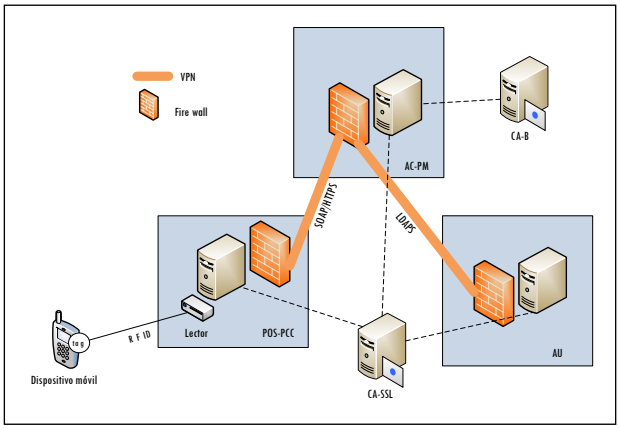
La seguridad es uno de los aspectos críticos en la arquitectura de facturación y pago. La seguridad de un sistema depende tanto de factores técnicos como de las políticas que implementen las entidades participantes, así como los usuarios mismos. Desde el punto de vista técnico, las pruebas demostraron que la arquitectura es segura si se adiciona un elemento que no se había considerado inicialmente como lo es el *firewall* en los módulos de administrador de cuentas y administrador de usuarios. Este *firewall* eleva la seguridad en el sistema, pero no lo hace invulnerable, ya que técnicas como el cifrado protegen la información, pero pueden ser violadas por personas expertas.

Otro punto importante son las entidades certificadoras, las cuales deben cumplir con todos los requerimientos que para ellas se exigen (Certicamara, 2007) y tener un nivel de aceptación tal que todas las partes que intervienen en el proceso confíen en ellas.

Desde el punto de vista tecnológico, el sistema se diseñó con un alto porcentaje de seguridad, pero aun así en las pruebas se detectaron posibles vulnerabilidades que pueden ocasionar suplantación de alguna de las partes, denegación del servicio o alteración del funcionamiento de algunos de los servidores. Por esta razón se implementaron medidas adicionales como *firewalls* y VPN. El diseño final del sistema se muestra en la Figura 6.

A pesar de los esquemas de seguridad implementados, si no existen políticas de protección en las entidades participantes, como los usuarios, los vendedores, los administradores del servicio, entre otros, el sistema podrá vulnerarse fácilmente.

Figura 6. Esquema final de seguridad



Fuente: presentación propia de los autores.

5. Conclusiones

- En materia de infraestructura y de *software* se cuenta con las herramientas necesarias para empezar a desarrollar la computación ubicua. En Colombia, a pesar de no ser un país con el más alto grado de desarrollo tecnológico, es factible el desarrollo de servicios en este campo, y la arquitectura propuesta en este trabajo es una muestra de ello.

- La gran penetración de la telefonía celular, especialmente en los estratos socioeconómicos más bajos, brinda buenas posibilidades para el desarrollo de servicios basados en dispositivos móviles. El acceso a este tipo de servicios por los sectores menos favorecidos será un aporte al programa de cierre de la brecha digital.

- La plataforma de facturación y pago se adapta a la legislación colombiana de comercio electrónico, ya que tiene su base en entidades de certificación y firmas digitales, mecanismos que se usaron en la plataforma para implementar los esquemas de seguridad. De esta manera este trabajo es una muestra de la aplicabilidad y de posibilidad de implementación de lo establecido en la ley colombiana.

- Colombia cuenta con la infraestructura necesaria para implementar servicios novedosos basados en la computación ubicua o la computación móvil, pues

se tiene una gran cobertura de telefonía celular, proveedores de servicios de banda ancha —los cuales cada vez son más apetecidos por los usuarios— y operadores de telecomunicaciones que están actualizando su tecnología con redes de próxima generación. Todo ello evidencia la posibilidad, desde el punto de vista tecnológico, de la implementación de la arquitectura propuesta.

Referencias

ALBIN, S. *The art of software architecture: design methods and techniques*. New York: John Wiley & Sons, 2003.

ASSA ABLOY. *Iclass, tag dataste: tag inteligente adhesivo sin contacto* [documento en línea]. 2007. <http://www.hidglobal.com/documents/iclass_tag_ds_es.pdf> [Consulta: 12-10-2008].

—. *iCLASS: serial protocol interface versión 2.4* [documento en línea]. 2006. <http://www.mastersbg.com/bg/partners/data/HID/pdf/iclass_rw100_300_400.pdf> [Consulta: 15-11-2008].

BODDUPALLI, P.; AL-BIN-ALI, F.; DAVIES, N. *et al*. Payment support in ubiquitous computing environments. *Mobile Computing Systems and Applications*. 2003, pp. 110-120.

CERTICÁMARA S. A. *Introducción al servicio digital de Certicámara* [web en línea]. 2007. <http://www.certicamara.com> [Consulta: 12-10-2008].

COLLABNET. *Discover metro: Metro Web Service Stack Overview* [documento en línea]. 2007. <https://metro.dev.java.net/discover/> [Consulta: 12-9-2008].

COLOMBIA. Ley 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones [documento en línea]. *Diario Oficial*. 18 de agosto de 1999, núm. 43673 <http://www.secretariasenado.gov.co/senado/basedoc/ley/1999/ley_0527_1999.html> [Consulta: 25-1-2009].

DAVIES, N. y GELLERSEN, H. Beyond prototypes: challenges in deploying ubiquitous systems. *IEEE Pervasive Computing*. 2002, vol. 1 núm. 1. pp. 26-35.

GAO, J.; CAI, J.; PATEL, K. y SHIM, S. A wireless payment system. Documento procedente de la *Second International Conference on Embedded Software and Systems*, 2005, pp. 367-374.

HODGES, J. y MORGAN, R. Lightweight Directory Access Protocol (v3): technical specification. *Internet Engineering Task Force, RFC 3377*. Septiembre, 2002.

INNOVISSION, RESEARCHS AND TECHNOLOGY. *Near field communication in the real world: turning the NFC promise into profitable, everyday applications* [documento en línea]. 2006. <http://www.kstinternational.com/download/paper/200601/IRT_NFC_white_paper_I___FINAL.doc> [Consulta 8-9-2008].

JUNIPER RESEARCH. *The big micropayment opportunity* [web en línea]. 2004 <http://juniperresearch.com/shop/viewwhitepaper.php?whitepaper=32> [Consulta: 10-10-2008].

KADHIWAL, S. Analysis of mobile payment security measures and different standards. *Computer Fraud & Security*. 2007, núm. 6, pp. 12-16.

LABROU, Y.; AGRE, J.; JI, L.; MOLINA, J.; CHEN, W.-I. Wireless wallet. Documento procedente de la *First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*. 2004, pp. 32-41.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY. *Keio University Schema for the SOAP/1.1 envelope. W3C* [web en línea]. 2001 <http://schemas.xmlsoap.org/soap/envelope/> [Consulta: 16-11-2008].

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO y BANCOLDEX. *Banca de Oportunidades: Cumbre Regional de Microcrédito para América Latina y el Caribe* [web en línea]. <http://www.bancadelasoportunidades.gov.co/index.htm> 2008. [Consulta: 10-10-2008].

MOBYPAY. *Sistema de pago por móvil* [web en línea]. 2008. <http://www.mobipay.es> [Consulta: 9-10-2008].

R. MOROZ LTD. *Understanding radio frequency identification (RFID)* [web en línea]. 2004. <http://www.rmoroz.com/rfid.html> [Consulta: 8-9-2008].

OBJECT XP. *jSMS User's guide* [documento en línea]. 2006. <http://www.objectxp.com/src/jsms/users_guide.pdf> [Consulta 12-9-2008].

PAYPAL [web en línea]. <https://www.paypal.com/us/cgi-bin/webscr?cmd=xpt/cps/mobile/MobileWaysToUse-outside> [Consulta: 9-10-2008].

TITANICLINUX.NET: DAOGEN. *Data Access Object (DAO) Code Generator version 2.4.1* [web en línea] <http://www.titaniclinux.net/daogen> [Consulta: 14-9-2008].

VILMOS, A. y KARNOUSKOS, S. *SEMOPS: design of a new payment service*. Documento procedente de la *14th International Workshop on Database and Expert Systems Applications*, 2003.

WEISER, M. The computer for the twenty-first century. *Scientific American*. 1991, vol. 265, núm. 3, pp. 94-104.